

Sm@rtCafé® Expert 64

The Java™-based smart card





Cost-effective and flexible through Java™



The Sm@rtCafé® Expert 64 from Giesecke & Devrient (G&D) offers a future-proof concept. Due to the Java Card™ operating system it has several advantages compared to conventional smart cards. In practice this means simplified implementation and economical operation with maximum flexibility and security.

There are already a great number of proven and cost-effective infrastructures for Java™ cards, in which the Sm@rtCafé® Expert 64 can be excellently integrated. The integration of comparable conventional cards, on the other hand, involves increased

adaptation requirements. With Java™ cards from G&D you can get your card system up and running fast.

G&D has an excellent reputation world-wide as an experienced security provider. In the healthcare sector G&D has provided 24 million ITSEC evaluated Java™ cards in Taiwan. All of the security requirements of the customer have been fulfilled. G&D's extensive experience with highly secure smart cards facilitates confident decision-making.

Thanks to the standardised post issuance function for

applets, cards in the field can be updated securely and easily. Additional applets can be added to the card, existing applets can be modified or deleted. As a result of the "Write once, run anywhere" concept for the use of G&D's Sm@rtCafé® Expert 64, you save costs and increase your investment security for years to come. By using firewalls, you can run applications securely and separately. Do you want, for example, to implement your own crypto-algorithm? You can do so easily with a post-issued applet. Sm@rtCafé® Expert 64 is the ideal multi-application card.

Sm@rtCafé® Expert 64 combines the advantages of innovative developments on one platform





G&D – Competence with security

G&D has already proven its competence in implementing smart card projects world-wide. Governments, banks, telecommunications enterprises as well as industrial companies are among our customers. They all profit from the flexibility and innovative power of a technology partner whose core competencies have always included making products secure. G&D provides you with successful support from the planning phase, through implementation, all the way to actual operation.

There are numerous areas of application and usage for Sm@rtCafé® Expert 64: for access control as well as for secure storage of personal data or as ID card, Sm@rtCafé® Expert 64 is the first choice for governments and enterprises.

The Sm@rtCafé® Expert 64 service range

Sm@rtCafé® Expert 64 complies completely with the SUN Java Card™ specifications. In addition, the operating system corresponds to the specifications of GlobalPlatform, ISO 7816 and EMV. This ensures the functionality of existing applications and infrastructures with Sm@rtCafé® Expert 64. Integration of the card in existing projects, seen from a cost efficiency perspective as well as that of multi-functionality, is simple with Sm@rtCafé® Expert 64.

Functionality and security were the focus during the development of Sm@rtCafé® Expert 64. Many security algorithms and functions are available. Thanks to the ingenious interplay of software and hardware security and G&D's dedication to always remaining a step ahead of the attackers, Sm@rtCafé® Expert 64 is one of the most secure operating systems on the market. Of course, this also applies to the known attacks SPA, DPA and DFA (e.g. light attacks).

Sm@rtCafé® Expert 64 supports the complete Java Card™ API as well as the Open Platform API. Optional features such as Multiple Security Domains, Delegated Management and DAP Verification are fully available. As a result, it is possible, for instance, for the card issuer to transfer security and administration services for its own applets to the application provider. In addition, Multiple Security Domains allow for the development of a trustworthy area on the card, which is fully available to the application provider.

The Bio API defined by the Java Card Forum enables the standardised access to G&D's own Match-on-Card algorithms implemented on the card. We can also implement manufacturer-independent algorithms without problems.

Sm@rtCafé® Expert 64 offers the customer the opportunity to activate applets already contained in the ROM or integrate applets provided by the customer in the ROM. This makes it possible to free up valuable EEPROM space, use more functions and reduce overall costs.



Additional G&D services

G&D offers its customers additional services for Sm@rtCafé® Expert 64 to keep the effort involved in programming, installation and personalisation to a minimum:

- Development of applications according to customer requirements
- Applications in ROM/EEPROM
- Personalisation of applications
- Integrated solutions for card personalisation

Sm@rtCafé® Expert 64 cards are supported by G&D's StarSign® Token for loading the corresponding PKI applets. This makes the cards usable in a greatest possible selection of PC applications on the most varied platforms. In addition, our card is also supported by the appropriate PKI applet from ActivCard Gold™.

Technical Data

Security:

- Symmetric encryption:
 - DES, 3DES, AES
- Asymmetric encryption:
 - RSA up to 2048 bit
 - DSA up to 1024 bit
- RSA on-card key generation up to 2048 bit
- DSA on-card key generation
- Hash algorithms MD5, SHA-1, RIPEMD-160
- Digital signatures with symmetric encryption
 - DES Mac, ISO 9797M1, ISO 9797M2, PKCS#5
 - AES Mac
- Digital signatures with asymmetric encryption
 - RSA with SHA-1, PKCS#1, RFC2409
 - RSA with MD5, PKCS#1, RFC2409
 - RSA with RIPEMD-160, ISO 9796, PKCS#1
 - DSA with SHA-1, FIPS 186-2 DSS
- DAP Verification
 - Multiple
 - Mandated
 - Using RSA or 3DES
- Cryptographic algorithms are secure against:
 - SPA
 - DPA
 - DFA (e.g. light attacks)
- Firewall for application separation is secure against:
 - DFA
 - Software attacks
- Security Domains
- Encrypted storage of confidential data (PINs, keys, etc.)

Technical Data

Chip:

- 16 bit High-Security Micro-Controller
- Common Criteria EAL 4+ certified

Memory:

64 kByte EEPROM

Specifications:

- GlobalPlatform Card Specification 2.0.1'
- SUN Java Card™ 2.2 incl. complete implementation of optional features, e.g. object deletion support, support of logical channels
- ISO 7816 1–5
- SUN Java Card™ 2.2 Bio API

Interfaces:

- Supports T=0 and T=1
- PTS/PPS
- Baud rate up to 115 kBaud

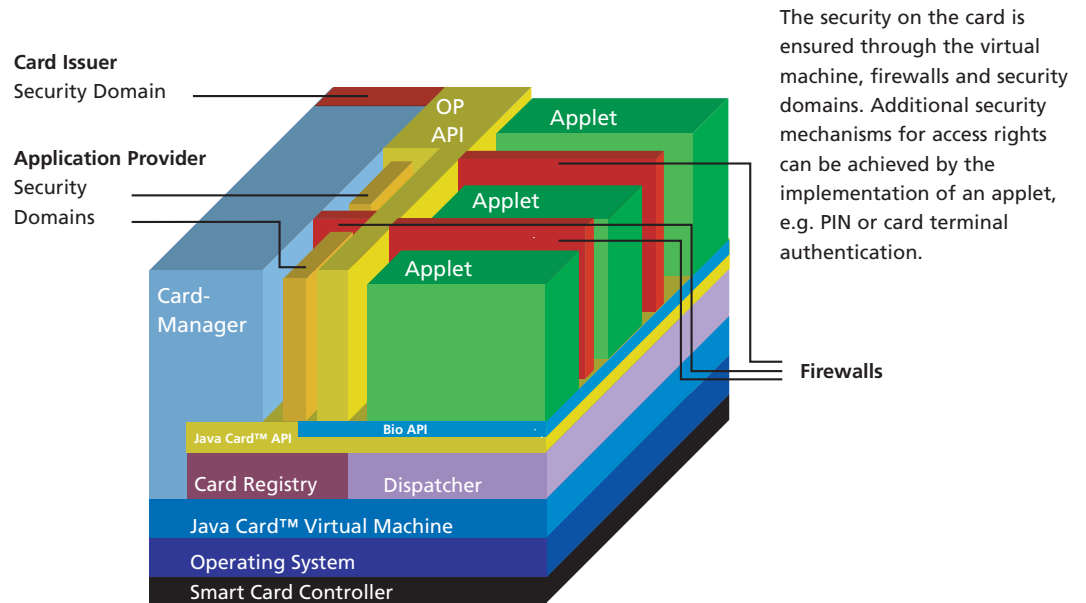
Compatible middleware:

- StarSign® Token for Java™
- ActivCard Gold™
- AET Safesign

Available applets:

- Identification
- PKI (Public Key Infrastructure)
- Healthcare
 - Doctor card
 - Patient card
- One-time password
- Loyalty
- Additional applications on request

The Architecture of the Sm@rtCafé® Expert 64



Features

- Memory management
 - Garbage collection
 - Defragmentation
 - Secure deletion of applets
 - Dynamic memory allocation
- Security certification
 - FIPS 140-2, Level 3
- 32 bit integer support
- Java Card™ RMI – enables distributed applications between terminal and card
- Biometric API
- Delegated Management
- Global PIN
- Additional commands for:
 - Common deletion of applications and Java Card™ packages
- Deletion of the Card Manager
- Card reset
- G&D Biometric MoC (Match-on-Card) and other implementations
- Available form factors:
 - Card
 - Module
 - Die
 - USB token

Glossary

- | | | |
|--|--|--|
| <p>Applet:
Java™ application</p> | <p>DPA:
Differential Power Analysis</p> | <p>Post Issuance:
Subsequent loading of applications in the field</p> |
| <p>API:
Application Programmers Interface</p> | <p>EEPROM:
Freely available user memory</p> | <p>ROM:
Fixed value memory, Read Only Memory</p> |
| <p>DAP:
Data Authentication Pattern</p> | <p>EMV:
Europay Mastercard Visa</p> | <p>SPA:
Simple Power Analysis</p> |
| <p>DFA:
Differential Fault Analysis</p> | <p>ITSEC:
Information Technology Security</p> | |

Giesecke & Devrient GmbH
Prinzregentenstrasse 159
P.O. Box 80 07 29
81607 Munich
GERMANY

Phone: +49 (0)89 41 19-19 57
Fax: +49 (0)89 41 19-27 78

indgov.cards@de.gi-de.com
www.gi-de.com

© Giesecke & Devrient GmbH, 2004
Sm@rtCafé® and StarSign® are registered
trademarks of Giesecke & Devrient GmbH. Java™
and Java Card™ are registered trademarks of Sun
Microsystems, Inc. ActivCard Gold™ is a registe-
red trademark of Activ Card. All technical data
subject to change without notice. G&D/GAO
Patents.

RDN 10/04E 1.000 Art.- Nr. 3000 665 ZDC



Giesecke & Devrient